

AES:LHE
F. #2018R02001

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
EMAIL ADDRESS info@forexnpower.com
THAT IS STORED AT PREMISES
CONTROLLED BY GOOGLE, INC.,

TO BE FILED UNDER SEAL

**APPLICATION FOR
SEARCH WARRANTS FOR
INFORMATION IN
POSSESSION OF PROVIDERS**
(info@forexnpower.com)

Case No. __18-M-613__

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH WARRANTS**

I, Keith McLaughlin, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for search warrants for information associated with the email address info@forexnpower.com (the “Subject Email Address”) that is stored at premises controlled by Google, Inc. (“Google”), an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I have been a Special Agent with the FBI for approximately 16 months. During my tenure with the FBI, I have participated in several white collar fraud investigations and have participated in all aspects of investigations, including conducting surveillance, executing search warrants, debriefing defendants and informants, interviewing witnesses, reviewing and analyzing recorded conversations, and analyzing telephone toll information. I am aware that white collar criminals commonly use electronic means of communication in furtherance of their criminal activities, including but not limited to electronic mail ("email"). As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

3. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from: (a) my personal participation in this investigation, (b) reports made to me by other law enforcement authorities, (c) information obtained from confidential sources of information, (d) interviews with witnesses and victims, and (e) review of certain emails, and other records and reports.¹

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of (a) wire fraud, (b) securities fraud, (c) investment adviser fraud, and (e) conspiring to commit these offenses, all in violation of Title 18, United States Code, Sections 371, 1343, 1349 and 2, and Title 15, United States Code, Sections

¹ Any conversations and email communications described below have been described in substance and in part.

78j(b) and 78ff (hereinafter collectively referred to as the “Target Offenses”) have been committed by Tae Hung Kang, also known as “Kevin Kang,” and John Won, and others known and as yet unknown. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband or fruits of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrants because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

7. The FBI is currently investigating the Target Offenses. As a result of that investigation, which remains ongoing, on or about April 11, 2018, a federal grand jury in the Eastern District of New York returned an indictment (the “Indictment”) charging Kang and Won with conspiracy to commit securities fraud, conspiracy to commit wire fraud, wire fraud, and money laundering conspiracy. See United States v. Kang, et al., No. 18-CR-184 (RJD). The Indictment is attached hereto as Exhibit A.

8. As alleged in the Indictment, in or about and between October 2010 and December 2013, Tae Hung Kang and John Won, together with others, engaged in two separate but related schemes: (i) a scheme to defraud investors and prospective investors in foreign exchange (“FX”) trading accounts managed by Kang and Won’s company, FOREXNPOWER, and (ii) a scheme to defraud investors and prospective investors in stock issued by Safety Capital Inc. (“Safety Capital”), a New York corporation that did business as FOREXNPOWER. With

respect to the first scheme, in or about and between October 2010 and December 2013, Kang and Won, together with others, solicited investors to open and deposit money into FX trading accounts in which trading decisions would be made by Kang, Won and their staff at FOREXNPOWER. In connection with this scheme, Kang and Won, together with others, defrauded investors in the managed FX trading accounts through material misrepresentations and omissions relating to, among other things: (1) the experience and expertise of FOREXNPOWER's trading staff; (2) the rates of return historically achieved by FOREXNPOWER; (3) likely future rates of return that would be achieved by FOREXNPOWER's computerized trading system, also known as "ASET" or "Super Power Bot;" (4) the general risk of FX trading; and (5) an insurance program FOREXNPOWER purported to maintain, which Kang and Won claimed would pay investors back for any losses they incurred, plus a ten percent profit. Indictment ¶ 14.

9. With respect to the second scheme, as is further alleged in the Indictment, from approximately July 2011 to July 2013, Kang and Won solicited investments into Safety Capital. Kang and Won generally told investors their capital would be pooled and used to conduct foreign exchange trading, though certain investors were told the money would be used to expand FOREXNPOWER to branch offices in other states. Kang and Won together with others, solicited over \$700,000 worth of investments Safety Capital stock. Only approximately \$3,000 was deposited into FX trading accounts. The majority of the investors' money was misappropriated by Won and Kang, through his wife, Sungmi Kang, who, together with Won, had signing authority over the Safety Capital bank accounts. Indictment ¶¶ 29-37.

USE OF THE SUBJECT EMAIL ACCOUNT

10. Based on my training, experience and knowledge of this investigation, as discussed in more detail below, I believe that Kang, Wong and others have used, among other things, e-mail communications to accomplish the unlawful activity described in the Indictment.

11. Specifically, the Subject Email Address was used to solicit investors and to communicate material misstatements to current investors.² For example, on or about August 17, 2012, an email was sent from the Subject Email Address in which the author stated that while some account holders were concerned about recent losses in their accounts, Safety Capital / FOREXNPOWER had its own insurance fund, and would pay investors back a ten percent profit on top of their initial investments. In order to take advantage of that insurance, however, investors would have to keep their money invested with FOREXNPOWER for at least one year. The email further stated “our ASET system will meet your financial goal at the end of the 60-kilometer marathon.” This email was false. First, this investigation has yielded no evidence the described insurance fund ever existed (such as bank accounts in which a fund similar to that described was maintained, and not a single FOREXNPOWER investor ever received reimbursement of their losses plus a ten percent profit. Moreover, at the time this email was written, the ASET system, which purported to make trading decisions based on computerized algorithm, had failed to generate profitable monthly returns.

12. Similarly, on or about November 7, 2012, an email was sent from the Subject Email Address to FOREXNPOWER investors. This time, Kang signed the email with his name. In this email, Kang apologized to investors for recent losses, and explained that they had a new

² Excerpts of email correspondence paraphrased or quoted herein refer to English language translations of email correspondence originally written in Korean.

“Skepler” system for trading that would generate monthly returns of 20 to 30 percent. No system generating such returns was ever used by FOREXNPOWER, and no FOREXNPOWER investor earned monthly returns in that range. In this email, Kang again reminded investors about the purported insurance program and said that no one would lose any of the money they had invested in FOREXNPOWER’s managed trading accounts. In reality, all of the FOREXNPOWER investors lost money.

13. As part of the instant investigation, I have reviewed records received from internet hosting service GoDaddy.com relating to various websites maintained by FOREXNPOWER. Those records reflect that on or about May 30, 2012, a sales representative from GoDaddy.com spoke with a male who represented himself to be named “Sungmi Kang.” The sales representative promoted GoDaddy.com’s free email service, and the male identifying himself as “Sungmi Kang” advised that his company already had free email service through Gmail, an email service provided by Google.

14. Based on my experience with internet email service providers, I am aware that Google offers email services to companies and individuals who wish to use an email address with a custom domain name.

15. On April 24, 2018, a preservation request letter for records relating to the Subject Email Address was sent to Google. In general, an email that is sent to a Google subscriber is stored in the subscriber’s “mail box” on Google servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google’s servers for a certain period of time.

BACKGROUND CONCERNING EMAIL

16. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail (“email”) access, to the public. Subscribers obtain an account by registering with Google. During the registration process, Google ask subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

17. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

18. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber’s full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users. Based on my training and my experience, I

know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

19. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

20. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

21. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct

under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crimes under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

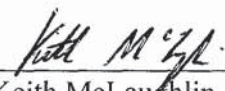
CONCLUSION

22. Based on the forgoing, I request that the Court issue the proposed search warrants. Because the warrants will be served on Google who will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

REQUEST FOR SEALING


23. I further request that the Court order that all papers in support of this application, including the affidavit and search warrants, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation, the scope of which is not known to all of the subjects of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give subjects an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,



Keith McLaughlin
Special Agent, FBI

Subscribed and sworn to before me on July ___, 2018



Honorable Ramon E. Reyes, Jr.
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with info@forexnpower.com that is stored at premises controlled by Google, Inc. (“Google”), a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google, Inc. (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on April 24, 2018, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 371, 1341, 1343, 1348, 1349, 1956 and 2, as well as Title 15, United States Code, Sections 78j(b) and 78ff, those violations involving Tae Hung Kang, also known as “Kevin Kang,” Sungmi Kang, John Won and any co-conspirators occurring after January 1, 2011 and before December 31, 2013, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) The fraudulent scheme to promote Safety Capital and FOREXNPOWER, recruit investors to use the foreign exchange accounts offered by FOREXNPOWER or invest in the securities of Safety Capital and FOREXNPOWER, communicate with current or former investors in either the foreign exchange trading accounts or Safety Capital and FOREXNPOWER securities, and/or launder the proceeds of those schemes using, inter alia, offshore bank and brokerage accounts;
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the email account owner;
- (c) Evidence indicating the email account owner’s state of mind as it relates to the crimes under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (e) The identity of the person(s) who communicated with the user ID about matters relating to the fraudulent scheme to promote Safety Capital and

FOREXNPOWER, recruit investors to use the foreign exchange accounts offered by FOREXNPOWER or invest in the securities of Safety Capital and FOREXNPOWER, communicate with current or former investors in either the foreign exchange trading accounts or FOREXNPOWER and Safety Capital securities, and/or launder the proceeds of those schemes using, inter alia, offshore bank and brokerage accounts, including records that help reveal their whereabouts.

EXHIBIT A

JMK:LHE
F. #2017R02001

FILED
IN CLERK'S OFFICE
U.S. DISTRICT COURT E.D.N.Y.
★ APR 11 2018 ★
BROOKLYN OFFICE

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

-----X

UNITED STATES OF AMERICA

- against -

TAE HUNG KANG,
also known as "Kevin Kang," and
JOHN WON,

Defendants.

-----X

THE GRAND JURY CHARGES:

INDICTMENT

CR 18 - 00184

Cr. No. (T. 15, U.S.C., §§ 78j(b) and 78ff; T. 18,
U.S.C., §§ 371, 981(a)(1)(C), 982(a)(1),
982(b)(1), 1343, 1349, 1956(h), 2 and
3551 et seq.; T. 21, U.S.C., § 853(p);
T. 28, U.S.C., § 2461(c))

KUNTZ, J.
LEVY, M.J.

INTRODUCTION

At all times relevant to this Indictment, unless otherwise indicated:

I. The Defendants and Relevant Individual

1. The defendant TAE HUNG KANG, also known as "Kevin Kang," was the founder and Chief Executive Officer of Safety Capital Management, Inc. ("Safety Capital").
2. The defendant JOHN WON was the President of GNS Capital Inc. ("GNS") and the Vice President and Secretary of Safety Capital. From on or about June 27, 2013 through the date of this Indictment, WON was listed by the National Futures Association ("NFA") as a principal and owner of GNS. Between August 2013 and February 2014, WON was registered with the Commodities Futures Trading Commission ("CFTC") as an associated person and branch manager of a registered introducing broker.

3. Jane Doe #1, an individual whose identity is known to the Grand Jury, was the President of Safety Capital and Vice President of GNS. During the relevant period, Jane Doe #1 acted at the direction of the defendant TAE HUNG KANG in connection with the events described herein.

II. The Relevant Entities

4. Safety Capital was a New York corporation with its principal place of business in Bayside, New York, and did business as "FOREXNPOWER." FOREXNPOWER was engaged in the foreign exchange ("FX") trading business. Specifically, Safety Capital, as FOREXNPOWER, purported to (1) provide training and education to individual investors seeking to learn how to trade foreign currencies; and (2) conduct FX trading on behalf of investor clients by applying special expertise and secret algorithmic trading methods called "ASET" or "Super Power-Bot."

5. GNS was a New York corporation with its principal place of business in Bayside, New York, at the same address as Safety Capital. GNS also did business as "FOREXNPOWER," and purported to engage in the same business activities as Safety Capital.

6. FX Clearing Company #1, a company the identity of which is known to the Grand Jury, was a New York-based international corporation that provided FX trading accounts and clearing services for individuals and entities engaged in FX trading. During the relevant period, FX Clearing Company #1 hosted accounts and cleared FX transactions on behalf of Safety Capital and GNS.

7. Introducing Broker #1, a company the identity of which is known to the Grand Jury, was a Charlotte, North Carolina-based corporation that was registered with the NFA

as an introducing broker. From approximately February 2012 to December 2013, Introducing Broker #1 served as an introducing broker for FOREXNPOWER clients.

III. Relevant Definitions

8. “FX trading” referred to the practice of trading one currency for another currency, e.g., the United States Dollar for the Pound Sterling, the currency of the United Kingdom.

9. A “security” was, among other things, any note, stock, bond, debenture, evidence of indebtedness, investment contract or participation in any profit-sharing agreement.

10. A Percentage Allocation Management Model (“PAMM”) account was an FX trading account that allowed investors to trade collectively using the same strategy and then receive a proportionate allocation of the profits and losses.

11. An FX “commodity trading adviser” (“FX CTA”) was an individual or organization that, for compensation or profit, advised others, directly or indirectly, as to the value or advisability of buying or selling FX.

12. An “introducing broker” was an individual or organization that solicited or accepted orders to buy or sell, among other things, foreign currencies, but did not accept money or other assets from customers to support these orders.

13. An “associated person” of an introducing broker was an individual who solicited orders, customers or customer funds on behalf of an introducing broker.

IV. The Fraudulent Schemes

A. The FX Trading Scheme

14. In or about and between October 2010 and December 2013, the defendants TAE HUNG KANG and JOHN WON, together with others, engaged in a scheme to defraud

investors and potential investors in FX trading accounts managed by FOREXNPOWER through material misrepresentations and omissions relating to, among other things: (1) the experience and expertise of FOREXNPOWER's trading staff; (2) the rates of return historically achieved by FOREXNPOWER; (3) likely future rates of return that would be achieved by FOREXNPOWER's computerized trading system, also known as "ASET" or "Super Power Bot;" (4) the general risk of FX trading; and (5) an insurance program FOREXNPOWER purported to maintain, which the defendants claimed would pay investors back for any losses they incurred, plus a 10 percent profit.

15. From approximately October 2010 through December 2013, the defendants TAE HUNG KANG and JOHN WON operated FOREXNPOWER. FOREXNPOWER conducted periodic seminars at its offices in Bayside, New York and in hotels in the New York City area, at which KANG, WON and others would present to potential investors about the mechanics of the FX market and how to make money through FX trading. KANG and WON, as well as other FOREXNPOWER staff, also pitched potential investors regarding the opportunity to open FX trading accounts with FX Clearing Company #1 that would be managed by FOREXNPOWER staff, who would then execute trades through a PAMM account.

16. At the seminars, the defendants TAE HUNG KANG and JOHN WON, together with others, represented to investors and potential investors that KANG was an expert in FX trading, and that trading using FOREXNPOWER's methods would generate a very profitable rate of return. For example, at a seminar held on or about April 20, 2012, which was attended by WON, KANG told potential investors that through his training they would "learn the 'know-how' to enjoy the life of comfort lounging on the beaches of the Bahamas and Hawaii . . . in a

year or two, or two to three years at most.” KANG further represented at the April 20, 2012 seminar that it was his belief that none of the participants in the seminars would ever lose a dollar.

17. In furtherance of the fraudulent scheme, the defendants TAE HUNG KANG and JOHN WON, together with others, disseminated and caused to be disseminated promotional material touting the investment opportunities available through FOREXNPOWER. Among other things, the promotional materials took the form of: (1) advertisements placed in Korean language newspapers and aired on Korean language radio; (2) brochures and pamphlets distributed at, among other places, FOREXNPOWER’s promotional seminars; and (3) emails distributed to lists of contacts maintained by the defendants.

18. The promotional materials contained numerous material misrepresentations and omissions. For example, in or around February 2012, an advertisement promoting FOREXNPOWER was published in a Korean language publication. The advertisement claimed that FOREXNPOWER provided an “easy trading method anyone can learn,” a “secret trading method generating more than 10% monthly profit,” and that the company “target[ed] \$100,000 with \$500 starting money.” Another advertisement provided details about FOREXNPOWER’s ASET trading product, claiming that it would “manage your account safely while you’re asleep or not home,” and that the purpose of the ASET accounts was “to make \$1 million and more within three to five years.” This advertisement specified that using ASET to trade would result in an estimated profit of 12 percent.

19. Contrary to the representations made at the seminars and in the promotional materials, the defendants TAE HUNG KANG and JOHN WON had very little expertise or experience in FX trading, and KANG, WON and FOREXNPOWER’S staff had not

historically achieved the touted profits through FX trading. Indeed, none of the defendants' customers obtained 10 percent monthly profits. Moreover, the algorithmic programs referred to as ASET and Super Power Bot had consistently failed to generate a profit through FX trading, and KANG and WON were aware that the programs consistently generated losses.

20. Through the fraudulent misrepresentations and omissions, the defendants TAE HUNG KANG and JOHN WON enticed at least 50 investors to invest over \$845,000 with FOREXNPOWER in managed FX trading accounts. FOREXNPOWER earned monthly fees generally in the amount of two percent of the value of accounts it managed and 30 percent of any profits generated by these accounts.

21. After investors opened their managed FX trading accounts with FOREXNPOWER, they received additional misleading communications from the defendant TAE HUNG KANG and others at FOREXNPOWER, in which they explained away losses in the investors' accounts and made false promises that the losses would be recouped. For example, on or about August 17, 2012, an individual using the email address "info@forexnpower.com" sent an email to FOREXNPOWER investors in which the individual wrote that while some account holders were concerned about recent losses in their accounts, Safety Capital had its own insurance fund, and would pay investors back 10 percent profit on top of their initial investments, but that investors had to keep their money invested with FOREXNPOWER for at least a year in order to take advantage of the insurance. This email further stated that "our ASET system will meet your financial goal at the end of the 60-kilometer marathon."

22. On or about November 7, 2012, the defendant TAE HUNG KANG sent an email from the info@forexnpower.com email address to FOREXNPOWER investors, in which he apologized for recent losses, but explained that the losses were caused because

FOREXNPOWER had not previously been using a “Skepler” system to trade, which would be “more profitable” going forward. KANG further explained that, by using the “Skepler” system, FOREXNPOWER would generate monthly returns of 20 to 30 percent for investors. KANG also reminded investors in the email about the insurance referred to in the August 17, 2012 email, and said that no one would lose any of the money they had invested in FOREXNPOWER’s managed trading accounts.

23. To facilitate the fraudulent scheme, the defendant JOHN WON served as the point of contact between FOREXNPOWER and FX Clearing Company #1 and Introducing Broker #1. On or about July 26, 2011, WON enabled FOREXNPOWER to begin engaging in FX trading on behalf of investors by facilitating the opening of an “exempt money manager” account in the name of Safety Capital with FX Clearing Company #1. Because FOREXNPOWER was not registered with the NFA as an FX CTA, FX Clearing Company #1 permitted FOREXNPOWER to introduce only up to 15 investors to participate in a PAMM account. Approximately five investors initially participated in the Safety Capital PAMM account. These investors invested approximately \$147,000 via the Safety Capital PAMM account. None of these investors earned a profit on their investments. Collectively, the investors lost approximately \$52,000.

24. On or about December 7, 2011, a representative from FX Clearing Company #1 sent an email to the defendant JOHN WON stating that FX Clearing Company #1 had suspended the Safety Capital PAMM account “because of the [sic] trading loss ratio to account equity was too high,” and that “to re-establish the PAMM we will need to see recent trading results that can show a positive trend.”

25. In approximately January 2012, the defendant JOHN WON informed a representative at FX Clearing Company #1 that he was starting a new FX money manager business under the name GNS. WON claimed that GNS had no relationship to Safety Capital. In an email sent on or about March 17, 2012, WON further represented to the FX Clearing Company #1 representative that he had “successfully acquired a BOT program,” that would conduct algorithmic trading, and acknowledged it may not “accumulate 800% in a year or so . . . [but] it is the most honest and less ‘risky.’” WON further represented that he had “10clients [sic] whom have demo account going to live accounts but we don’t want any ties to Safety capital. It is imperative I don’t run into any further delay for our clients.” In reality and contrary to these representations, and as WON was fully aware, GNS was jointly controlled by KANG and WON, and GNS and Safety Capital were effectively interchangeable entities continuing to conduct business as FOREXNPOWER.

26. Following the suspension of the Safety Capital PAMM account, the defendant JOHN WON opened a new PAMM account in the name of GNS with FX Clearing Company #1 on or about March 28, 2012. Approximately eight additional investors participated in the GNS PAMM account.

27. Starting in approximately April 2012, the defendants TAE HUNG KANG and JOHN WON began opening additional FX trading accounts through the use of Introducing Broker #1. The purpose of opening accounts through Introducing Broker #1 was to allow FOREXNPOWER to have more than 15 customer accounts open at FX Clearing Company #1, despite not being registered as an FX CTA. Introducing brokers at FX Clearing Company #1 were entitled to receive a commission payment that amounted to a percentage of trades. WON negotiated an arrangement with Introducing Broker #1 pursuant to which that commission was

split between Introducing Broker #1 and FOREXNPOWER. KANG and WON obtained over \$620,000 in investments into FX trading accounts opened by investors through Introducing Broker #1. Those investors incurred collective losses of over \$334,000.

28. In total, investors into FX trading accounts managed by FOREXNPOWER invested approximately \$845,000 and lost nearly \$400,000, including commissions and fees. No investor received the full refund plus 10% payment from FOREXNPOWER's touted insurance fund in the wake of these losses.

B. The Stock Investment Scheme

29. In addition to the fraudulent scheme set forth above, the defendants TAE HUNG KANG and JOHN WON, together with others, also perpetrated a related fraudulent scheme involving direct investment into Safety Capital.

30. From approximately July 2011 to July 2013, the defendants TAE HUNG KANG and JOHN WON solicited investments into Safety Capital by selling Safety Capital stock. The stock was not registered with the United States Securities and Exchange Commission. In connection with the sale of this stock, KANG and WON perpetrated a scheme to defraud investors and potential investors through material misrepresentations and omissions relating to the intended use of investor funds. KANG made a variety of representations to investors and potential investors regarding how the funds invested in the company would be used, but most investors were told that their money would be pooled by FOREXNPOWER to conduct FX trading. In reality, KANG and WON misappropriated the majority of the money.

31. For example, in approximately March 2012, Investor #1, an individual whose identity is known to the Grand Jury, saw an advertisement for FOREXNPOWER and attended several seminars hosted by FOREXNPOWER in Bayside, New York, at which the

defendant TAE HUNG KANG presented about FX trading. During one of these presentations KANG advised that while the Korean community did not traditionally invest in the FX market, if the attendees invested with KANG and took advantage of FOREXNPOWER's ASET trading method, the return on their investments would be substantial within a few years.

32. On or about July 24, 2012, Investor #1 met with the defendants TAE HUNG KANG and JOHN WON and Jane Doe #1 at KANG's office in Bayside, New York in order to invest in Safety Capital. At that meeting, Investor #1 provided KANG with a check for \$50,000 in exchange for 25 shares of Safety Capital stock. This amount of money represented the majority of Investor #1's life savings. During the meeting, KANG explained to Investor #1 that the value of Safety Capital stock would increase exponentially in the future. When Investor #1 signed the check for \$50,000 to purchase Safety Capital stock, KANG, WON and Jane Doe #1 broke into applause. In or around October 2012, Investor #1 changed his mind and asked KANG for his money back. KANG told Investor #1 that he was waiting for an incoming investment from a new investor, and then would be able to refund Investor #1's investment. KANG later promised to buy back Investor #1's stake, but Investor #1 never received any money from KANG.

33. In or around and between July and August 2013, the defendant TAE HUNG KANG also solicited a total of approximately \$70,000 in investments in Safety Capital stock from Investor #2, an individual whose identity is known to the Grand Jury. During meetings to discuss the investment, KANG told Investor #2 that it was his intention to expand FOREXNPOWER into branch offices in several states, and that Investor #2's investment would be used to open the first branch office in Fort Lee, New Jersey. He also told Investor #2 that she would receive a monthly dividend of four and a half percent of her investment. Investor #2 made

an original investment of \$20,000 in or around July 2013, and received a dividend payment of \$800 (four percent of the original investment) from Safety Capital approximately one month later. Investor #2 then made additional investments totaling \$50,000, but received no further dividend payments.

34. The defendant JOHN WON was also involved in pitching investors to purchase Safety Capital stock. For example, in or around June 2013, the defendant TAE HUNG KANG met with another potential investor, Investor #3, an individual whose identity is known to the Grand Jury, at FOREXNPOWER's office in Bayside, New York. During that meeting, KANG explained that Investor #3's investment would be used to conduct FX trading, and that any profit generated by his investment would be split between Investor #3 and FOREXNPOWER. Several days later, Investor #3 returned to FOREXNPOWER's office, where he met with WON. During that meeting, WON told Investor #3 about the potential for significant profit from investing in the FX market through FOREXNPOWER. In approximately July 2013, Investor #3 invested approximately \$10,000 in Safety Capital in exchange for 20 shares of stock.

35. In total, the defendants TAE HUNG KANG and JOHN WON solicited approximately \$718,000 dollars in investments in Safety Capital stock. This money was deposited into bank accounts held in the name of Safety Capital and GNS. WON and Jane Doe #1 collectively maintained exclusive signing authority over those accounts. Only approximately \$3,000 of incoming investor funds were transferred to FX trading accounts. The majority of the total investment in Safety Capital stock was spent in the form of checks payable to WON and Jane Doe #1 and on personal expenses on behalf of KANG, WON and Jane Doe #1.

36. As an illustrative example of the flow of money through these accounts, on or about July 25, 2013, a check in the amount of \$30,000 from an account held by Investor #2 was deposited into a bank account in Bayside, New York in the name of Safety Capital (the "SC Account"), as to which Jane Doe #1 held exclusive signing authority. On or about July 28, 2013, Jane Doe #1 wrote a check in the amount of \$19,000 to GNS from the SC Account, which was then deposited into a bank account in Bayside, New York in the name of GNS (the "GNS Account"), as to which the defendant JOHN WON and Jane Doe #1 jointly held exclusive signing authority. On or about July 30, 2013, WON wrote a check in the amount of \$7,000 to himself from the GNS Account. An additional \$7,000 was withdrawn in cash from the GNS Account by Jane Doe #1 on or about August 2, 2013.

37. Other than token payments, purportedly representing dividends or profits, made by FOREXNPOWER to certain investors, the investors in Safety Capital stock lost their entire investments as a result of the scheme, resulting in a total of over \$700,000 in losses.

COUNT ONE

(Wire Fraud Conspiracy – FX Trading Scheme)

38. The allegations contained in paragraphs one through 37 are realleged and incorporated as if fully set forth in this paragraph.

39. In or about and between February 2012 and December 2013, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants TAE HUNG KANG, also known as "Kevin Kang," and JOHN WON, together with others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud one or more investors and potential investors in FX trading accounts managed by FOREXNPOWER, and to obtain money and property from them by means of one or more materially false and

fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce writings, signs, signals, pictures and sounds, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

COUNT TWO

(Securities Fraud Conspiracy – Stock Investment Scheme)

40. The allegations contained in paragraphs one through 37 are realleged and incorporated as if fully set forth in this paragraph.

41. In or about and between July 2011 and July 2013, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants TAE HUNG KANG, also known as “Kevin Kang,” and JOHN WON, together with others, did knowingly and willfully conspire to use and employ one or more manipulative and deceptive devices and contrivances, contrary to Rule 10b-5 of the Rules and Regulations of the United States Securities and Exchange Commission, Title 17, Code of Federal Regulations, Section 240.10b-5, by: (i) employing one or more devices, schemes and artifices to defraud; (ii) making one or more untrue statements of material fact and omitting to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; and (iii) engaging in one or more acts, practices and courses of business which would and did operate as a fraud and deceit upon one or more investors and potential investors in Safety Capital, directly and indirectly, by use of means and instrumentalities of interstate commerce and the mails, contrary to Title 15, United States Code, Sections 78j(b) and 78ff.

42. In furtherance of the conspiracy and to effect its objects, within the Eastern District of New York and elsewhere, the defendants TAE HUNG KANG and JOHN WON, together with others, did commit and cause to be committed, among others, the following:

OVERT ACTS

(a) On or about January 9, 2013, KANG signed a stock purchase agreement with Investor #4, an individual whose identity is known to the Grand Jury, documenting her purchase of 1,000 shares of Safety Capital stock;

(b) On or about January 16, 2013, WON signed a check payable to himself drawn from the GNS account in the amount of \$5,000;

(c) On or about April 19, 2013, KANG signed a stock purchase agreement with Investor #5, an individual whose identity is known to the Grand Jury, documenting his purchase of 500 shares of Safety Capital stock;

(d) On or about July 3, 2013, KANG signed a stock purchase agreement with Investor #2 documenting her purchase of 1,000 shares of Safety Capital stock; and

(e) On or about July 30, 2013, WON signed a check payable to himself drawn from the GNS Account in the amount of \$7,000.

(Title 18, United States Code, Sections 371 and 3551 et seq.)

COUNT THREE

(Securities Fraud – Stock Investment Scheme)

43. The allegations set forth in paragraphs one through 37 are realleged and incorporated as if fully set forth in this paragraph.

44. In or about and between February 2012 and December 2013, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants TAE HUNG KANG, also known as “Kevin Kang,” and JOHN WON, together with others, did knowingly and willfully use and employ one or more manipulative and deceptive devices and contrivances, contrary to Rule 10b-5 of the Rules and Regulations of the United States Securities and Exchange Commission, Title 17, Code of Federal Regulations, Section 240.10b-5, by: (a) employing one or more devices, schemes and artifices to defraud; (b) making one or more untrue statements of material fact and omitting to state one or more material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; and (c) engaging in one or more acts, practices and courses of business which would and did operate as a fraud and deceit upon one or more investors and potential investors in Safety Capital, in connection with the purchase and sale of investments in Safety Capital, directly and indirectly, by use of means and instrumentalities of interstate commerce and the mails.

(Title 15, United States Code, Sections 78j(b) and 78ff; Title 18, United States Code, Sections 2 and 3551 et seq.)

COUNT FOUR

(Wire Fraud Conspiracy – Stock Investment Scheme)

45. The allegations set forth in paragraphs one through 37 are realleged and incorporated as if fully set forth in this paragraph.

46. In or about and between February 2012 and December 2013, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants TAE HUNG KANG, also known as “Kevin Kang,” and JOHN WON, together with

others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud one or more investors and potential investors in stock issued by Safety Capital, and to obtain money and property from them by means of one or more materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce writings, signs, signals, pictures and sounds, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

COUNT FIVE

(Wire Fraud – Stock Investment Scheme)

47. The allegations set forth in paragraphs one through 37 are realleged and incorporated as if fully set forth in this paragraph.

48. On or about August 1, 2013, within the Eastern District of New York, the defendant TAE HUNG KANG, also known as “Kevin Kang,” together with others, did knowingly and intentionally devise a scheme and artifice to defraud Investor #2, and to obtain money and property from Investor #2 by means of one or more materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, KANG transmitted and caused to be transmitted, by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, to wit: a wire transfer in the amount of \$30,000 from Investor #2’s bank account in New Jersey to the SC Account maintained in the Eastern District of New York.

(Title 18, United States Code, Sections 1343, 2 and 3551 et seq.)

COUNT SIX
(Money Laundering Conspiracy)

49. The allegations contained in paragraphs one through 37 are realleged and incorporated as if fully set forth in this paragraph.

50. In or about and between July 2011 and July 2013, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants TAE HUNG KANG, also known as "Kevin Kang," and JOHN WON, together with others, did knowingly and intentionally conspire to conduct one or more financial transactions in and affecting interstate and foreign commerce, to wit: checks and electronic payments, which transactions in fact involved the proceeds of one or more specified unlawful activities, to wit: wire fraud, in violation of Title 18, United States Code, Section 1343, and fraud in the sale of securities, in violation of Title 15, United States Code, Sections 78j(b) and 78ff, knowing that the property involved in such transactions represented the proceeds of some form of unlawful activity, and with the intent to promote the carrying on of said specified unlawful activities, contrary to Title 18, United States Code, Section 1956(a)(1)(A)(i).

(Title 18, United States Code, Sections 1956(h) and 3551 et seq.)

CRIMINAL FORFEITURE ALLEGATION AS TO
COUNTS ONE THROUGH FIVE

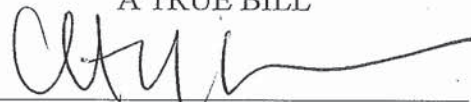
51. The United States hereby gives notice to the defendants that, upon their conviction of any of the offenses charged in Counts One through Five, the government will seek forfeiture in accordance with Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), which require any person convicted of such offenses to forfeit any property, real or personal, constituting or derived from proceeds obtained directly or indirectly as a result of such offenses.

- (c) has been placed beyond the jurisdiction of the court;
- (d) has been substantially diminished in value; or
- (e) has been commingled with other property which cannot be divided without difficulty;


it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1), to seek forfeiture of any other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 981(a)(1) and 982(b)(1); Title 21, United States Code, Section 853(p))

A TRUE BILL



FOREPERSON


RICHARD P. DONOGHUE
UNITED STATES ATTORNEY
EASTERN DISTRICT OF NEW YORK

